IP блок GstdR3432015_APBctr_AXIStrdflow

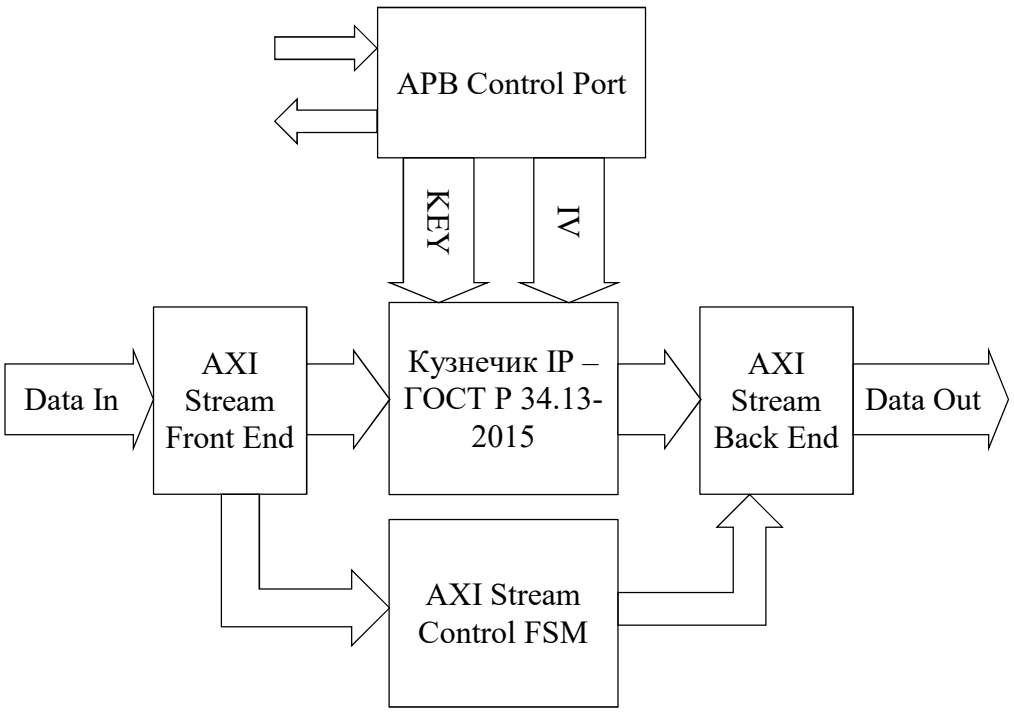
Назначение IP-блока

IP-блок предназначен для зашифровывания и расшифровывания данных в соответствии со стандартом ГОСТ Р 34.13-2015 в потоке AXI Stream с разрядностью от 8 до 128 бит.

Детали стандарта изложены в [1].

Структурная схема

Упрощённая структурная схема блока показана на рис.:



APB Control Port. Узел управления режимами через интерфейс APB [4]. Используется для загрузки ключей шифрования, начальных значений блоков (IV), смены режима зашифровывания, проверки текущего состояния IP-блока. В узле физически отсутствуют каналы пересылок информации, которые могли бы быть использованы для чтения информации об уже загруженном ключе.

AXI Stream Front End. Узел отработки протокола интерфейса AXI Stream [5] при приеме данных. Дополнительный функционал — преобразование ширины шины данных из допустимых в AXI Stream (от 8 бит до 128) в шину данных Кузнечик IP (128 бит, фиксированная).

AXI Stream Back End. Узел преобразования потока данных от узла зашифровывания/расшифровывания в интерфейс AXI Stream, с разрешенной шириной шины данных (от 8 до 128 бит).

AXI Stream Control FSM. Узел управления пересылками данных. Конечный автомат обеспечивает чтение данных из буферов Front End, обработку служебных сигналов Кузнечик IP, размещение данных в FIFO Back End и отработку протокола обмена по выходной шине AXI Stream.

Кузнечик IP – ГОСТ Р 34.13-2015 [3] — узел зашифровывания и расшифровывания данных в соответствии с алгоритмами ГОСТ Р 34.13-2015.

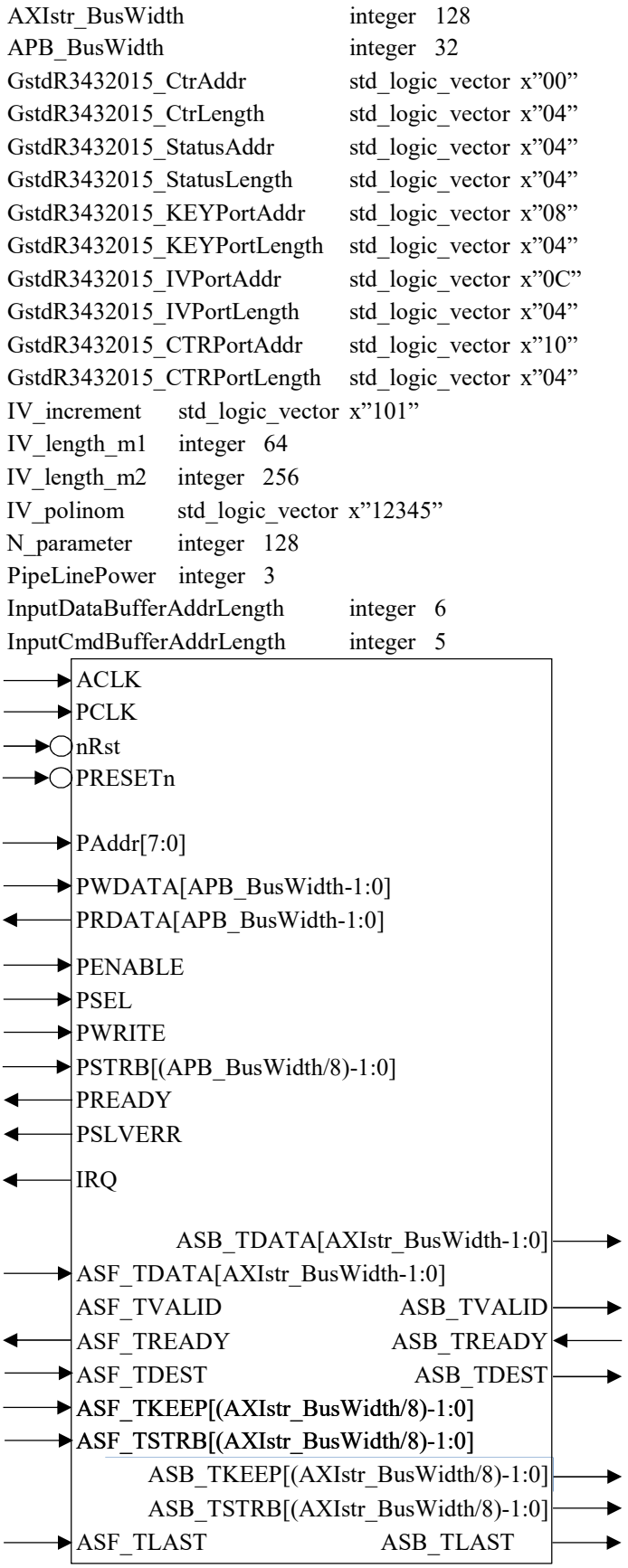
Узел Кузнечик IP реализует следующие режимы работы [2]:

— Режим простой замены;
— Режим гаммирования;
— Режим гаммирования с обратной связью по выходу;
— Режим простой замены с зацеплением;
— Режим гаммирования с обратной связью по шифртексту.

Развернутое описание режимов работы приведено в документах [2], [3].

Описание интерфейса

Условное графическое отображение IP-блока представлено на рис.



Назначения сигналов представлены в табл.:

Название	Направ-ление	Акт. уровень	Описание
Системные сигналы			
ACLK	in	↑	Тактовый сигнал интерфейса AXI Stream (Slave и Master), тактовый сигнал узла криптопреобразования (Кузнечик IP)
PCLK	in	↑	Тактовый сигнал интерфейса APB
nRst	in	‘0’	Системный сигнал перезапуска
PRESETn	in	‘0’	Сигнал перезапуска интерфейса APB
IRQ	out	‘1’	Сигнал прерывания для инициатора запроса по шине APB, активный уровень формируется при некоторых изменениях состояния IP-блока
Сигналы интерфейса APB			
PAddr	in	Addr	Адрес элемента доступа. Адресация побайтная, Потенциально доступно для доступа 256 байт.
PWDATA	in	Data	Данные для записи. Ширина шины данных зависит от параметра синтеза и может быть 8, 16 или 32 байта.
PRDATA	out	Data	Данные при чтении. Ширина шины данных зависит от параметра синтеза и может быть 8, 16 или 32 байта.
PENABLE	in	‘1’	Активный уровень означает прохождение второго и последующих циклов тактового сигнала при обращении к устройству.
PSEL	in	‘1’	Источник запроса генерирует активный уровень индивидуального сигнала PSEL при обращении к каждому устройству.
PWRITE	in	‘1’	Активный уровень означает обращение к устройству для записи.
PSTRB	in	‘1’	Строб разрешения пересылки отдельного байта в составе шины данных.
PREADY	out	‘1’	Сигнал готовности к обмену в данном обращении от устройства — приемника запроса.
PSLVERR	in	‘1’	Активный уровень означает ошибку доступа — не разрешенная для обмена зона адресного пространства.
Сигналы интерфейса AXI Stream (Slave)			
ASF_TDATA	in	Data	AXI Stream Front End Transmission Data. Данные, пересылаемые по интерфейсу AXI Stream. Допустимая ширина шины данных может быть 8,16,32,64 или 128 бит.
ASF_TVALID	in	‘1’	Признак валидности пересылаемых данных.
ASF_TREADY	out	‘1’	Признак готовности устройства к приёму данных
ASF_TDEST	in	–	Назначение пересылаемого пакета данных. Может принимать следующие значения: — ‘0’ – пересылается открытый текст, который будет зашифрован; — ‘1’ – пересылается зашифрованный текст, который будет расшифрован.
ASF_TKEEP	in	‘1’	Индикатор валидности содержимого соответствующего байта, пересылаемого по шине. [5, page 2-24]
ASF_TSTRB	in	‘1’	Индикатор валидности содержимого соответствующего байта, пересылаемого по шине. [5, page 2-24]
ASF_TLAST	in	‘1’	Признак последнего слова в пересылаемом пакете.
Сигналы интерфейса AXI Stream (Master)			
ASB_TDATA	out	Data	AXI Stream Back End Transmission Data. Данные, пересылаемые по интерфейсу AXI Stream. Допустимая ширина шины данных может быть 8,16,32,64 или 128 бит.
ASB_TVALID	out	‘1’	Признак валидности пересылаемых данных.
ASB_TREADY	in	‘1’	Признак готовности внешнего приемника устройства к приёму данных
ASB_TDEST	out	‘1’	Назначение пересылаемого пакета данных. Может принимать

Название	Направ-ление	Акт. уровень	Описание
			следующие значения: — ‘0’ – пересылается открытый текст; — ‘1’ – пересылается зашифрованный текст.
ASB_TKEEP	out	‘1’	Индикатор валидности содержимого соответствующего байта, пересылаемого по шине. [5, page 2-24]
ASB_TSTRB	out	‘1’	Индикатор валидности содержимого соответствующего байта, пересылаемого по шине. [5, page 2-24]
ASB_TLAST	out	‘1’	Признак последнего слова в пересылаемом пакете.

Любые более детальные описания сигналов шин APB и AXI Stream и логики их применения могут быть прочитаны только в официальных документах разработчика интерфейсов — [4],[5].

Параметры синтеза IP-блока представлены в табл:

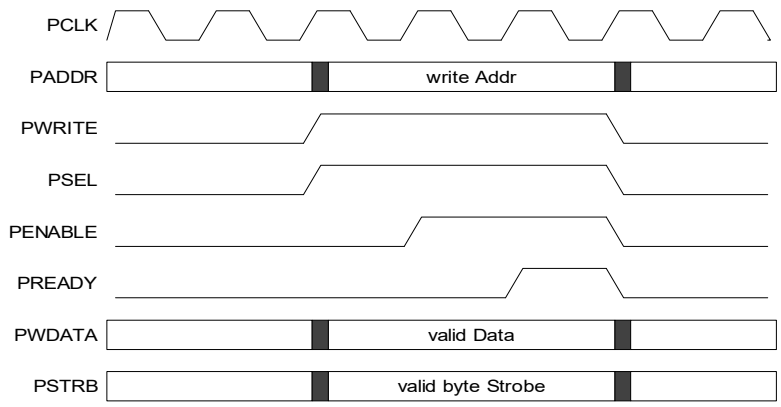
Название	По умолчанию	Описание
AXIstr_BusWidth	128	Ширина шины данных интерфейса AXI Stream. Параметр един как для входящего потока (AXI Stream Front End – ASF_xxx), так и для исходящего потока данных (AXI Stream Back End – ASB_xxx). Допустимые величины — 8,16,32,64,128.
APB_BusWidth	32	Ширина шины данных для интерфейса APB. Допустимые величины — 8,16,32.
GstdR3432015_CtrAddr	x”00”	Адрес размещения регистра управления IP-блоком.
GstdR3432015_CtrLength	x”04”	Длина адресной зоны размещения регистра управления IP-блока, в байтах.
GstdR3432015_StatusAddr	x”04”	Адрес размещения регистра состояния IP-блока.
GstdR3432015_StatusLength	x”04”	Длина адресной зоны размещения регистра состояния IP-блока, в байтах.
GstdR3432015_KEYPortAddr	x”08”	Адрес вершины стека размещения ключа шифрования.
GstdR3432015_KEYPortLength	x”04”	Длина вершины стека в байтах.
GstdR3432015_IVPortAddr	x”0C”	Адрес вершины стека размещения синхропосылки (IV).
GstdR3432015_IVPortLength	x”04”	Длина вершины стека размещения синхропосылки в байтах.
GstdR3432015_CTRPortAddr	x”10”	Адрес вершины стека чтения счётчика синхропосылки для режима гаммирования.
GstdR3432015_CTRPortLength	x”04”	Длина вершины стека чтения счётчика синхропосылки в байтах.
IV_increment	x”101”	Величина шага инкремента значения счётчика для режима гаммирования.
IV_length_m1	64	Длина счётчика CTR для режима гаммирования.
IV_length_m2	256	Длина синхропосылки (IV) для всех режимов, кроме простой замены и гаммирования.
IV_polinom	x”12345”	Полином для сдвигового регистра с обратной связью, используется в режиме гаммирования при альтернативном параметре изменения величины CTR [3].
N_parameter	128	Параметр n для вычисления очередной величины R_q во всех режимах, кроме простой замены и гаммирования [2, стр. 14,17,20]. Для режима гаммирования с обратной связью по шифртексту s = N_parameter.
PipeLinePower	3	Параметр вычисления длины конвейера обработки информации при зашифровывании и расшифровывании. Длина конвейера равна $2^{PipeLinePower}$. Чем длиннее конвейер, тем выше доступная тактовая частота обработки, и больше занимаемый IP-блоком объём логики.

Название	По умолчанию	Описание
InputDataBufferAddrLength	6	Длина шины адреса входного буфера данных шины AXI Stream. Объём буфера вычисляется как $N*2^{InputDataBufferAddrLength}$ байт, где N – ширина шины данных AXI Stream в байтах. Т.е., при 128 битной шине (16 байт) и параметре 6 объём входного буфера составит 1024 байта.
InputCmdBufferAddrLength	5	Длина шины адреса входного буфера команд конечного автомата управления (AXI Stream Control FSM). Определяет количество независимых блоков данных, которые могут быть приняты по AXI Stream в пределах входного буфера данных и обрабатываться в конвейерном режиме. Объём буфера команд вычисляется как $2^{InputCmdBufferAddrLength}$

Описание параметров активности сигналов интерфейса

Запись данных по интерфейсу APB

При записи служебной и управляющей информации используется интерфейс APB, позволяющий адресоваться к отдельным элементам хранения IP-блока. Одиночный цикл записи представлен на рис.:

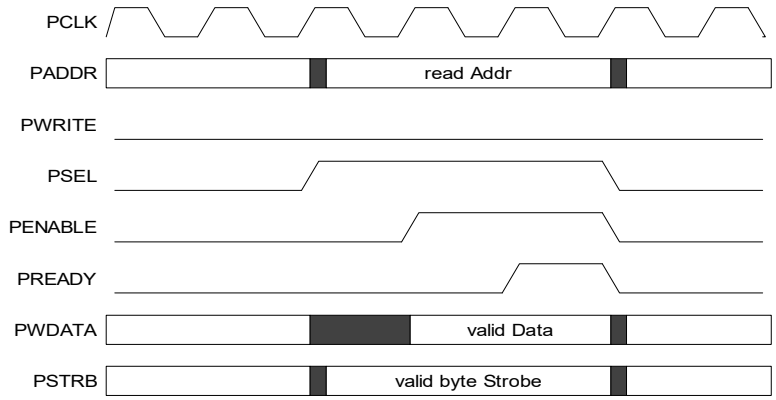


При правильном адресе обращения записаны будут только те байты, которые сопровождаются активным уровнем соответствующей линии PSTRB. К примеру, при записи двойного слова x”ABCDEF01” в сопровождении содержимого PSTRB = “1101” записаны будут только байты 3,2,0 (x”ABCD__01”).

При ширине шины данных интерфейса APB в 8 бит — для записи двойного слова регистра управления потребуется четыре последовательных обращения по адресам соответствующих байтов регистра.

Чтение данных по интерфейсу APB

Одиночный цикл чтения представлен на рис.:



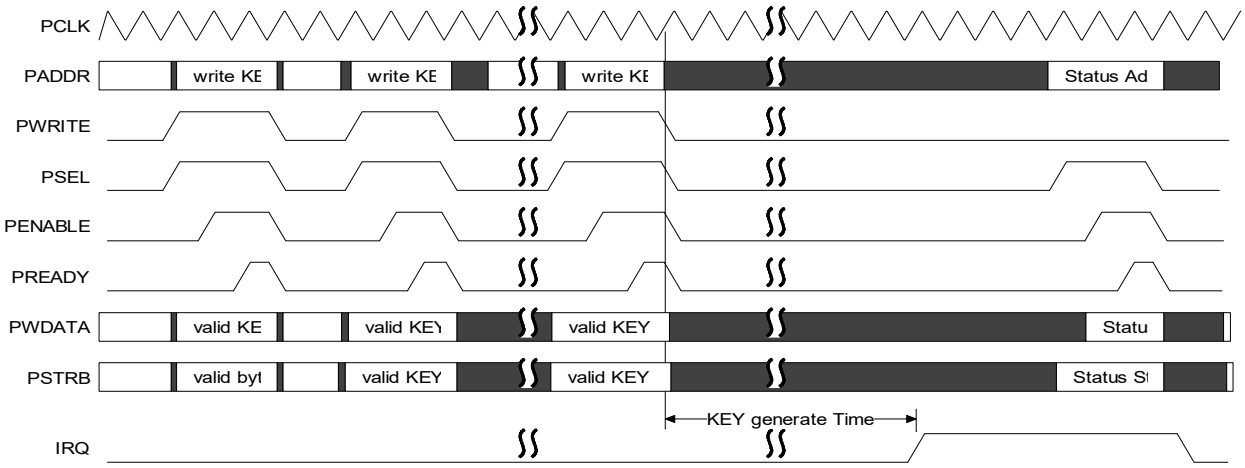
При правильном адресе обращения на шину данных будут выданы только те байты, которые сопровождаются активным уровнем соответствующей линии PSTRB. К примеру,

при чтении двойного слова в сопровождении содержимого PSTRB = “1011” реально прочитаны будут только байты 3,1,0. Позиции байтов, для которых PSTRB(i) = ‘0’ — заполняются нулями. Т.е., прочитано будет двойное слово x”98005432”.

При ширине шины данных интерфейса APB в 8 бит — для чтения двойного слова регистра состояния потребуется четыре последовательных обращения по адресам соответствующих байтов регистра.

Загрузка ключа (KEY) или начального значения (IV)

После загрузки ключа или начального значения необходимо подождать выработки сигнала прерывания IRQ. Снятие сигнала IRQ обеспечивается чтением регистра состояния устройства. После этого устройство будет готово к приему пакетов данных по шине AXI Stream. Загрузка ключа и отработка прерывания представлены на рис.:



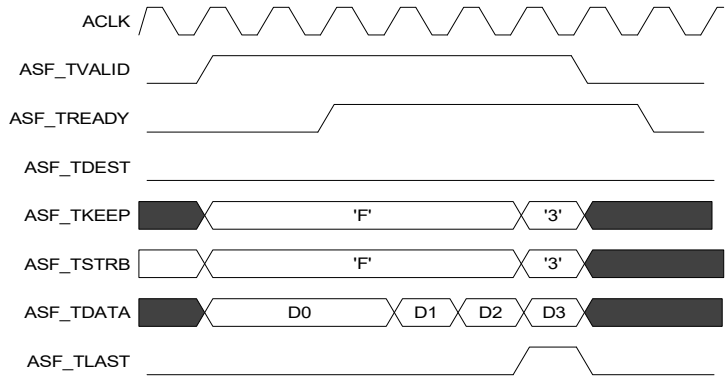
При длине ключа в 256 бит и ширине шины данных APB в 32 бита потребуется 8 циклов записи для полной загрузки ключа в порт записи. По истечении времени генерации внутреннего ключа будет сформировано прерывание. После очистки флага прерывания чтением регистра состояния устройство готово к работе с новым ключом шифрования.

Начальное значение (IV) загружается таким же образом в порт загрузки IV.

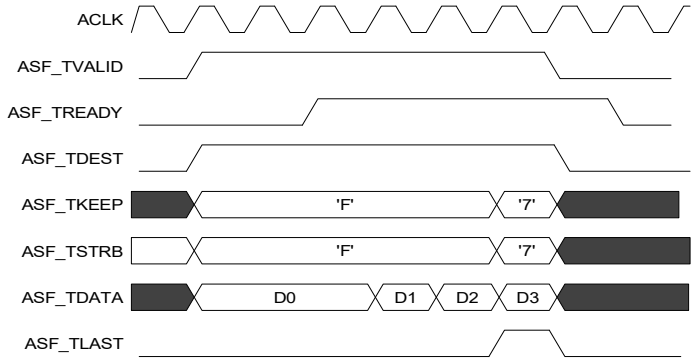
Загрузка блока данных по интерфейсу AXI Stream

Через интерфейс пересылаются два основных типа данных — зашифрованные и незашифрованные. Индикатором типа потока служит состояние сигнала ASF_DEST для входного потока и ASB_DEST для выходного потока данных.

Пересылка незашифрованного пакета данных, из 14 байт:



Пересылка зашифрованного пакета данных, из 15 байт:



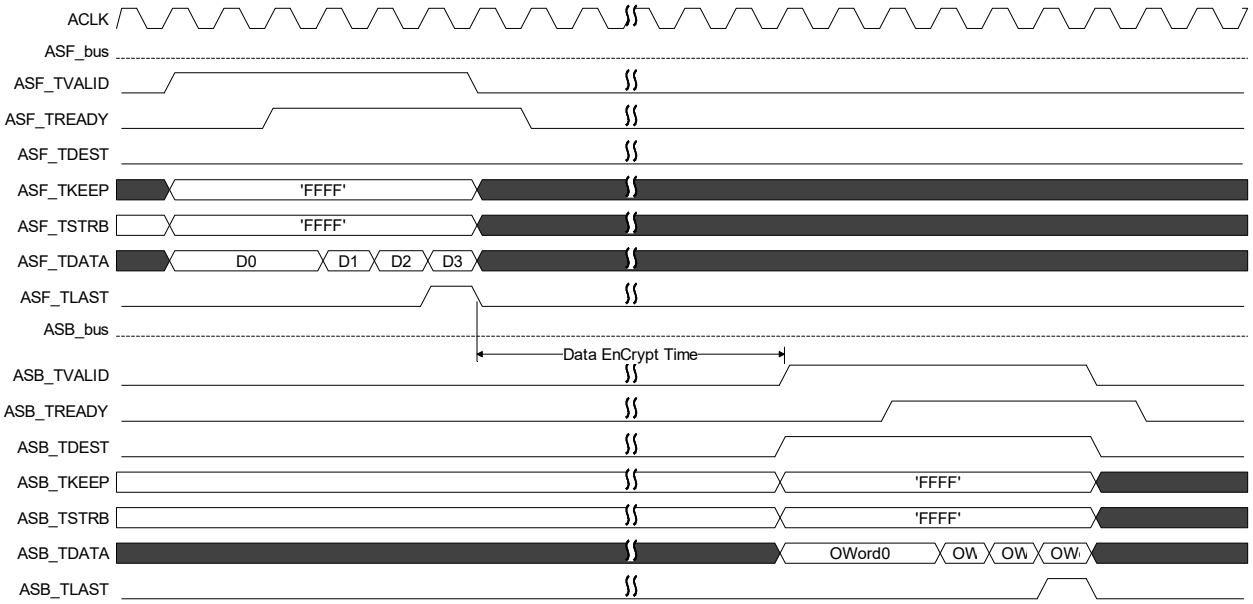
В зависимости от состояния сигнала ASF_TDEST внутренняя логика IP-блока обеспечивает либо зашифровывание принятого пакета данных, либо его расшифровывание.

Сигнал ASF_TSTRB служит для маскирования байт в потоке данных. Если ASF_TSRB(i), соответствующий байту на шине ASF_TDATA, равен нулю, то такой байт считается невалидным и его позиция в потоке данных заполняется нулями.

Логика IP-блока запоминает состояние только последнего ASF_TSTRB в потоке, при активном уровне ASF_TLAST. Все предыдущие значения ASF_TSTRB используются при подготовке данных, но не пересылаются на ASB_TSTRB.

Не рекомендуется посылать на шифрование пакеты данных, не кратные длине слова преобразования IP Кузнечик — 128 бит. В связи с особенностью работы ASF_TSTRB при не кратном 128 битам количестве возможна потеря части данных или невозможность последующего расшифрования.

Полный цикл обработки пакета из 4-х 128-битных слов представлен на рис.:



На стороне шины ASF данные обозначены как незашифрованные. На стороне шины ASB данные уже обозначены как зашифрованные и могут быть направлены в соответствующее место хранения.

Длительность Data EnCrypt Time зависит от тактовой частоты интерфейса, режима работы, количества данных и параметра синтеза конвейера обработки.

Адресная карта интерфейса APB

Адресная карта интерфейса APB представлена в табл.:

Адрес	Размер, байт	Название	Описание
x”00”	4	ControlReg	Регистр управления
x”04”	4	StatusReg	Регистр состояния
x”08”	4	KEYport	Порт записи ключа шифрования. Порт определен только для записи, при попытке чтения на шине данных отсутствует осмысленная информация.
x”0C”	4	IVport	Порт записи начального значения. Порт определён только для записи, при попытке чтения на шине данных отсутствует осмысленная информация.
x”10”	4	CTRport	Порт записи счётчика для режима гаммирования. При чтении читается последнее вычисленное значение счетчика.
x”14” — x”FF”	236	rsv	зарезервировано

ControlReg[31:0] — используется для управления режимами устройства. Состоит из следующих полей:

31 20	19 16	15 11	10	9 8	7 5	4	3 2	1	0
rsv	GM[3:0]	rsv	rsv	IVM[1:0]	rsv	CGU	rsv	CIP	CKP
R,x"000"	RW,'0'	R,x"0"	R,'0'	RW,'0'	R,'000'	RW,'0'	R,'00'	RW,'0'	RW,'0'

CKP — **C**lear **K**EY **p**ipe. Очистка конвейера ключа. При записи ‘1’ содержимое конвейера загрузки ключа очищается. Используется в тех случаях, когда запись ключа была начата, но по любым причинам не завершена до конца (до полной длины ключа). В этом случае информация из конвейера не перегружается в устройство зашифровывания и конвейер остаётся в промежуточном состоянии. Очистка конвейера приводит его в исходное состояние. Поле автоматически возвращается в ‘0’ после выполнения операции.

CIP — **C**lear **I**V **p**ipe. Очистка конвейера IV. При записи ‘1’ содержимое конвейера загрузки IV очищается. Используется в тех случаях, когда запись IV была начата, но по любым причинам не завершена до конца (до полной длины ключа). В этом случае информация из конвейера не перегружается в устройство зашифровывания и конвейер остаётся в промежуточном состоянии. Очистка конвейера приводит его в исходное состояние. Поле автоматически возвращается в ‘0’ после выполнения операции.

CGU — **C**lear **G**stdR3432015 **u**nit. Очистка IP-блока Кузнечик IP – ГОСТ Р 34.13-2015. При записи ‘1’ происходит аппаратный перезапуск IP-блока шифрования, с очисткой всех конвейеров, ключевой и служебной информацией. Поле автоматически возвращается в ‘0’ после выполнения операции.

IVM[1:0] — **IV** **M**ode. Вариант использования величины CTR в режиме гаммирования. Может принимать следующие значения:

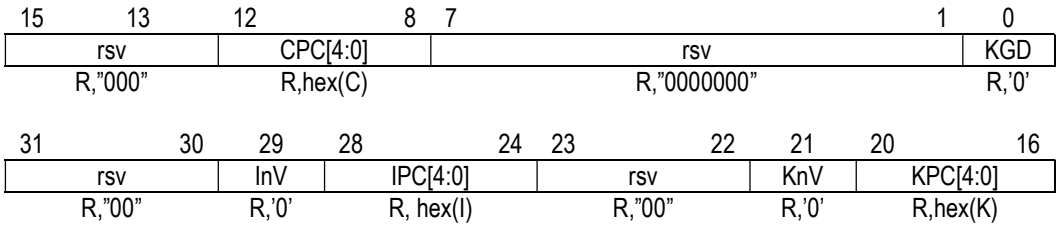
— 00 — стандартный режим счёта, величина CTR инкрементируется на каждом новом слове обрабатываемого блока данных.
— 01 — режим работы как сдвиговый регистр с обратной связью, используется совместно с полиномом IV_polinom из параметров синтеза [3].
— 10,11 — зарезервировано.

GM[3:0] — **G**amma **M**ode. Режим зашифровывания/расшифровывания. Может принимать следующие значения:

— 0000 — режим простой замены;
— 0001 — режим гаммирования;
— 0010 — режим гаммирования с обратной связью по выходу;
— 0011 — режим простой замены с зацеплением;
— 0100 — режим гаммирования с обратной связью по шифртексту;
— 0101 – 1111 — зарезервировано.

Не допускается смена режима во время обработки блока данных.

StatusReg[31:0] — используется для проверки текущего состояния устройства. Состоит из следующих полей:



KGD — **K**EY **G**enerate **D**one. Флаг завершения генерации внутреннего ключа шифрования. Состояние ‘1’ означает, что генерация внутреннего ключа на основе загруженной информации завершена. Поле читается после возникновения прерывания по завершении генерации. Очищается при чтении.

CPC — **C**TR **P**ipe **C**ount. Счётчик конвейера загрузки значения CTR, используемого в режиме гаммирования. Значение по умолчанию равно:

$$CPC = hex\left(\frac{128}{\text{APB\_BusWidth}} - 1\right),$$

т.е., шестнадцатиричному представлению отношения длины счётчика CTR к ширине шины APB минус 1. При ширине шины 32 бита значение поля по умолчанию будет равно 3. Любое меньшее значение означает, что в конвейер загрузки была загружена часть величины счётчика и загрузка не была завершена.

KPC — **K**EY **P**ipe **C**ount. Счётчик конвейера загрузки ключа. Значение по умолчанию равно:

$$KPC = hex\left(\frac{256}{\text{APB\_BusWidth}} - 1\right),$$

т.е., шестнадцатиричному представлению отношения длины ключа к ширине шины APB минус 1. При ширине шины 32 бита значение поля по умолчанию будет равно 7. Любое меньшее значение означает, что в конвейер загрузки была загружена часть данных ключа и загрузка не была завершена.

KnV — **K**EY **n**ot **V**alid. Флаг не валидности ключа шифрования. Возникает при попытке записи нового значения ключа по неправильному адресу. К примеру, при записи ключа по адресу 0x09 вместо 0x08.

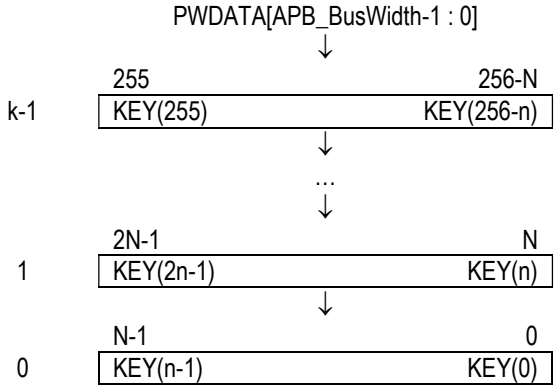
IPC — **I**V **P**ipe **C**ount. Счётчик конвейера загрузки IV. Значение по умолчанию равно:

$$IPC = hex\left(\frac{256}{\text{APB\_BusWidth}} - 1\right),$$

т.е., шестнадцатиричному представлению отношения длины IV к ширине шины APB минус 1. При ширине шины 32 бита значение поля по умолчанию будет равно 7. Любое меньшее значение означает, что в конвейер загрузки была загружена часть данных IV и загрузка не была завершена.

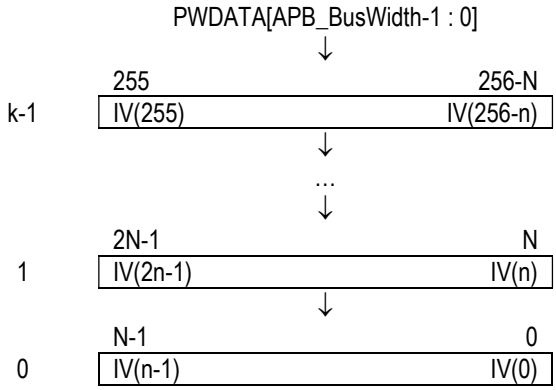
InV — **I**V **n**ot **V**alid. Флаг не валидности IV. Возникает при попытке записи нового значения IV по неправильному адресу. К примеру, при записи ключа по адресу 0x0E вместо 0x0C.

KEYport. Порт записи ключа шифрования. Представляет собой верхушку стека, длина которого и разрядность элементов зависит от ширины шины данных APB:



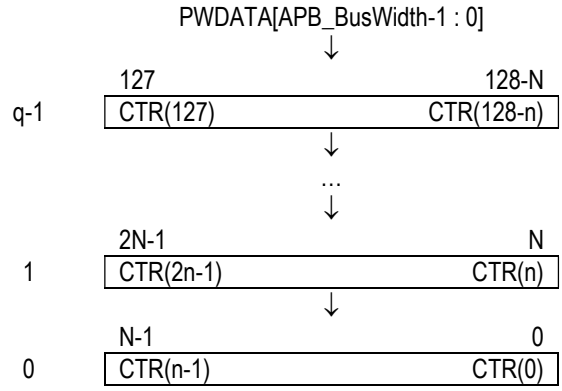
где N = APB_BusWidth, $k = \frac{256}{\text{APB\_BusWidth}}$. Загрузка ключа осуществляется младшими битами вперёд в верхушку стека. В процессе последовательных обращений на запись в порт записи ключа, ранее загруженные данные передвигаются по конвейеру стека до его полного заполнения. После этого ключ отправляется на IP-блок шифрования, и одновременно очищается содержимое конвейера стека. Аппаратные возможности для любого чтения элементов стека — отсутствуют в логике IP-блока.

IVport. Порт записи IV. Представляет собой верхушку стека, длина которого и разрядность элементов зависит от ширины шины данных APB:



где N = APB_BusWidth, $k = \frac{256}{\text{APB\_BusWidth}}$. Загрузка IV осуществляется младшими битами вперёд в верхушку стека. В процессе последовательных обращений на запись в порт записи IV, ранее загруженные данные передвигаются по конвейеру стека до его полного заполнения. После этого IV отправляется на IP-блок шифрования, и одновременно очищается содержимое конвейера стека. Аппаратные возможности для любого чтения элементов стека — отсутствуют в логике IP-блока.

CTRport. Порт записи начального значения счётчика CTR. Представляет собой верхушку стека, длина которого и разрядность элементов зависит от ширины шины данных APB:



где N = APB_BusWidth, $q = \frac{128}{\text{APB\_BusWidth}}$. Загрузка CTR осуществляется младшими битами вперёд в верхушку стека. В процессе последовательных обращений на запись в порт записи CTR, ранее загруженные данные передвигаются по конвейеру стека до его полного заполнения. После этого CTR отправляется на IP-блок шифрования, и одновременно очищается содержимое конвейера стека. Аппаратные возможности для любого чтения элементов стека — отсутствуют в логике IP-блока.

Для счётчика CTR существует возможность прочитать последнее вычисленное значение, которое будет использоваться как начальное при зашифровывании следующего блока данных.

Комплект поставки

В комплект поставки входят следующие файлы:

№	Файл	Тип	Описание
1	*GstdR3432015_APBctr_AXIStrdflow.vhd*	*VHDL*	Верхний уровень структуры IP-блока криптопреобразования информации
2	*Kuznechik_GstdR34132015_MMv01.vhd*	*VHDL*	Модуль криптопреобразования, реализующий алгоритмы и режимы криптопреобразования в соответствии с ГОСТ Р 34.13-2015
3	*FIFO_wyuxb_ryuxb_sclk.vhd*	*VHDL*	Параметризуемый модуль FIFO, для организации временного хранения данных и команд интерфейса.

Элементы сценария тестирования перечислены в табл.:

№	Элемент сценария	Прохож-дение	Примечание
1	*Запись данных в регистр управления*	√	*Запись произвольных данных, без контроля корректности управления устройством.*
2	*Запись управляющих параметров в регистр управления*	√	*Запись управляющих данных, с контролем корректности управления устройством.*
3	*Чтение регистра управления*	√	
4	*Чтение регистра состояния*	√	
5	*Загрузка ключа*	√	*Загружен ключ, определенный для тестов в [2]*
6	*Загрузка IV*	√	*Загружен IV, определенный для тестов в [2]*
7	*Загрузка CTR*	√	*Загружен CTR, определенный для тестов в [2]*
8	*Установка режима простой замены*	√	
9	*Зашифрован набор данных, определенный в [2]*	√	
10	*Расшифрован набор данных, определенный в [2]*	√	*Данные после расшифрования идентичны данным, зашифрованным в сценарии 9.*
11	*Установка режима гаммирования*	√	
12	*Зашифрован набор данных, определенный в [2]*	√	
13	*Расшифрован набор данных, определенный в [2]*	√	*Данные после расшифрования идентичны данным, зашифрованным в сценарии 12.*
14	*Установка режима гаммирования с обратной связью по выходу*	√	
15	*Зашифрован набор данных, определенный в [2]*	√	
16	*Расшифрован набор данных, определенный в [2]*	√	*Данные после расшифрования идентичны данным, зашифрованным в сценарии 15.*
17	*Установка режима простой замены с зацеплением*	√	
18	*Зашифрован набор данных, определенный в [2]*	√	
19	*Расшифрован набор данных, определенный в [2]*	√	*Данные после расшифрования идентичны данным, зашифрованным в сценарии 18.*
20	*Установка режима гаммирования с обратной связью по шифртексту*	√	
21	*Зашифрован набор данных, определенный в [2]*	√	
22	*Расшифрован набор данных, определенный в [2]*	√	*Данные после расшифрования идентичны данным, зашифрованным в сценарии 121.*

Отчёт о покрытии кода тестами

Покрытие кода тестовым сценарием:

```
Coverage Report Summary Data by file

================================================================================
=== File: E:/…/FIFO_wyuxb_ryuxb_sclk_behavior.vhd
================================================================================
    Enabled Coverage              Bins      Hits    Misses  Coverage
    ----------------              ----      ----    ------  --------
    Branches                        23        21         2    91.30%
    Conditions                       9         5         4    55.55%
    Statements                      45        45         0   100.00%
    Toggles                       1628       977       651    60.01%

================================================================================
=== File: E:/…/GstdR3432015_APBctr_AXIStrdflow_behavior.vhd
================================================================================
    Enabled Coverage              Bins      Hits    Misses  Coverage
    ----------------              ----      ----    ------  --------
    Branches                       362       339        23    93.64%
    Conditions                     145       115        30    79.31%
    Expressions                      5         4         1    80.00%
    FSM States                      11        11         0   100.00%
    FSM Transitions                 18        11         7    61.11%
    Statements                     330       315        15    95.45%
    Toggles                       6919      2912      4007    42.08%

================================================================================
=== File: E:/…/Kuznechik_GstdR34132015_MMv01_behavior.vhd
================================================================================
    Enabled Coverage              Bins      Hits    Misses  Coverage
    ----------------              ----      ----    ------  --------
    Branches                       275       266         9    96.72%
    Conditions                     100        75        25    75.00%
    Expressions                     15         9         6    60.00%
    Statements                     250       241         9    96.40%
    Toggles                       5444      3462      1982    63.59%

================================================================================
=== File: E:/…/gstdr3432015_apbctr_ahbdflow_tb_struct.vhd
================================================================================
    Enabled Coverage              Bins      Hits    Misses  Coverage
    ----------------              ----      ----    ------  --------
    Toggles                       1256      1030       226    82.00%

================================================================================
=== File: E:/…/gstdr3432015_apbctr_ahbdflow_tester_flow.vhd
================================================================================
    Enabled Coverage              Bins      Hits    Misses  Coverage
    ----------------              ----      ----    ------  --------
    Branches                        86        60        26    69.76%
    Conditions                       6         2         4    33.33%
    Statements                     647       613        34    94.74%
    Toggles                       2516      2064       452    82.03%
```

```
TOTAL ASSERTION COVERAGE: 100.00%  ASSERTIONS: 6

Total Coverage By File (code coverage only, filtered view): 78.29%
```

Моделирование режимов (*если требуются отдельные сценарии тестирования*)

Параметр “xxx” позволяет синтезировать IP-блок с…. Матрица прохождения тестов режимов при разных величинах параметра представлена в табл:

	Параметр синтеза						
Режим	0	1	…	…	…	…	n
0	√	√	√	√	√	√	√
…	×	×	×	√	√	√	×
k	√	√	√	√	√	√	√

0 — режим 0;

1 — режим 1;

… — режим …;

k — режим k;

Примечания по результатам прохождения (успешных, неуспешных, признанных приемлемыми).

Скоростные характеристики

Предельные скоростные характеристики IP-блока в зависимости от физической платформы синтеза проекта приведены в табл:

Физическая платформа	Изготовитель	Тактовая частота Clk, MHz	Объём логики		Объём памяти, бит (blocks)
			LUT	reg	

В колонках указываются значимые параметры и виды логического исполнения (LUT, базовые элементы логики в технологической библиотеке и т.п.)

Список литературы

1. ГОСТ Р 34.12─2015, КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ Блочные шифры, Москва, Стандартинформ 2015, УДК 681.3.06:006.354 ОКС 35. 040 ОКСТУ 5002 П85, http://www.gostinfo.ru/
2. ГОСТ Р 34.13─2015, КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ Режимы работы блочных шифров, Москва, Стандартинформ 2015, УДК 681.3.06:006.354 ОКС 35. 040 ОКСТУ 5002 П85, http://www.gostinfo.ru/
3. Кузнечик IP – ГОСТ Р 34.13-2015.
4. AMBA® APB Protocol Specification, Copyright © 2003-2023 Arm Ltd. All rights reserved. ARM IHI 0024E (ID022823), www.arm.com
5. AMBA® AXI-Stream Protocol Specification, Copyright © 2010, 2021 Arm Limited or its affiliates. All rights reserved. ARM IHI 0051B (ID040921), www.arm.com